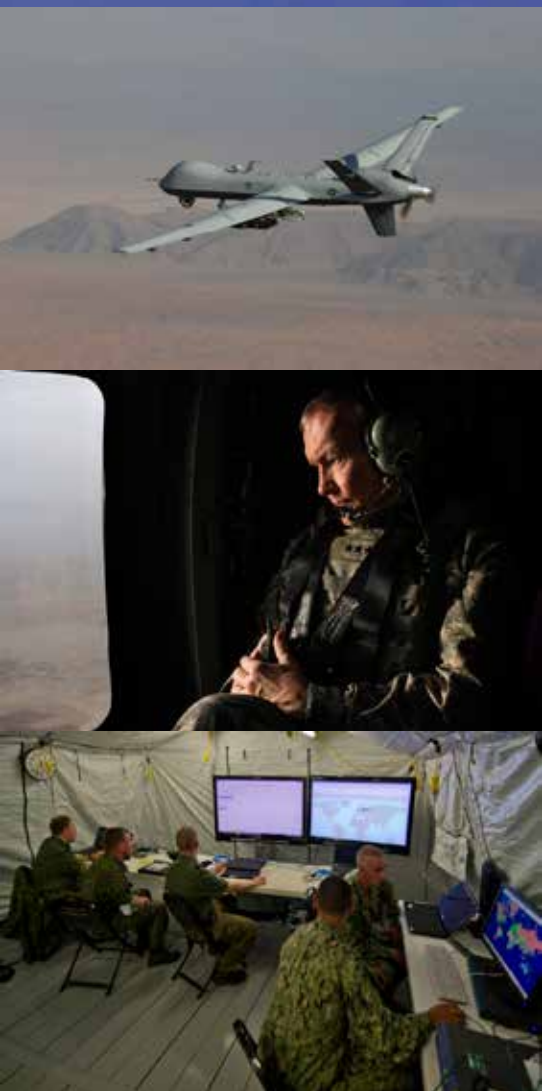


JOINT INFORMATION ENVIRONMENT

DEFENSE INFORMATION SYSTEMS AGENCY

STRATEGIC PLAN

2014 — 2019
VERSION 2

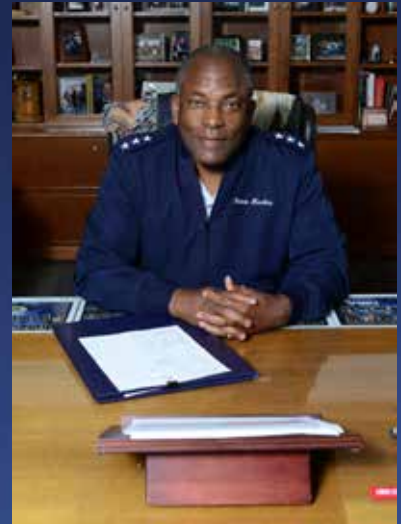


DISA
A COMBAT SUPPORT AGENCY

Director's Intent

Two years ago, I stated in our Strategic Plan that the Agency was at a crossroads. We were completing combat operations in Iraq, and anxiously looked to determine how we, as a nation, would conclude similar combat operations in Afghanistan. Words like “sequestration” and “cyber protection teams” were new to our lexicon, and we did not fully comprehend their effects within the Agency.

The crossroad is now in our rearview mirror, and cyber security and defense and the DoD Information Network (DoDIN) are now a central part of our daily operations as the premier IT Combat Support Agency. Our nation and our leadership have emphatically stated we must transition, as we conclude 13 years of war. Not only must we transition to a post-conflict and financially constrained era, but we must also transition into a smaller, yet equally lethal military. Our focus must be on cyberspace sovereignty, agility, and innovation, given its more dominant role today.



The 2015 Fiscal Year budgets, presented by the President and Secretary of Defense, highlights focus areas for our Agency for the next 3-5 years. The Quadrennial Defense Review, released in March 2014, also highlights the Agency's need to meet its cyber mission with a dynamic and professional workforce. The Secretary of Defense stated, "We will rebalance our military over the next decade and put it on a sustainable path to protect and advance U.S. interests and America's global leadership." The Chairman of the Joint Chiefs of Staff stated in his "2nd Term Strategic Direction to the Joint Force" that "Our investments in cyber and a new Joint Information Environment are changing how we fight and defend the Nation." DISA will play a vital role in this rebalancing effort, cyber, and the Joint Information Environment.

There is no other workforce in the Department of Defense better postured to deliver cyberspace sovereignty effects across the entire battlespace continuum (from peace to conflict) than the men and women of the Defense Information Systems Agency. We must be readily cognizant of, and leaders in, cyberspace operations, by being the experts in the DoD Strategy for Operating in Cyberspace (DSOC), the DoD Strategy for Defending Networks, Systems, and Data (DDNSD), and exploiting the DoD Cyberspace Workforce Strategy.

Our workforce must be agile and willingly adapt to new requirements. The days of being only a telecommunications Agency have passed. This new era reinforces the need to maintain a vigilant "focus" on our broad Strategic Goals of (1) Evolve the Joint Information Environment, (2) Provide Joint Command and Control and Leadership Support, (3) Operate and Assure the DISA Information Enterprise as part of the DoD Information Networks (DoDIN), and (4) Optimize Department Investments.



More specifically, we need to:

- Develop and implement an integrated intelligence-driven analytical and data-driven defensive cyber operations campaign to enhance defense in depth, the Cyber Kill Chain, and response to Advanced Persistent Threats. This includes internal heuristics where the cyber posture of the Enterprise is continuously analyzed, audited, and inspected ensuring DoDIN users adhere to the highest standards of C2, daily operations, and cyber hygiene. DISA will uphold a standard of excellence in this area where the employment, operations, and maintenance of the DoDIN is a conscious decision vigorously exercised daily.
- Develop and mature the DoD mobile ecosystem where tablets and mobile devices become the status quo delivering secure and unclassified capabilities, data, and applications.
- Lead the DoD in teaming with industry to build out the DoD public and private clouds, while recognizing the implied and explicit security expectations from DoD senior leadership.
- Reorient the Agency in a purposeful and strategic manner, to be more agile and responsive to a dynamic “IT Enterprise,” thus requiring operational and tactical shifts in our organizational and personnel alignment.
- Lead the DoD in optimizing data center consolidation through the establishment of Core Data Centers centered around industry best practice standards and dis-establishment of obsolete, fiscally unaffordable centers. Where and when feasible, capitalize on commercial cloud solutions that support application modernization while maintaining DoD security guidelines/standards.
- Establish a core capability for DoD to realize efficiencies through application rationalization, accomplished through a systematic process of identifying opportunities for consolidation, modernization and the sun setting of legacy systems.
- Enhance Customer Relationship Management (CRM) processes focused on automating, to the maximum extent possible, the requirements management and fulfillment components of our services. This ensures a consistent and singular approach to addressing mission partner requirements across the Agency.
- Institutionalize a culture of IT shared services both internal and external to the Agency. We can no longer operate multiple, stove-pipe operations and capabilities at the expense of the Agency as a whole. Neither can we, as the DoD’s leader in IT, continue to unnecessarily build and house multiple one-off IT capabilities.
- Craft an acquisition and budgeting process in 2014, responsive to the needs of our mission partners, while still being the unrivaled leader in IT acquisitions, procurements, and budgeting. We must modernize acquisition and budgeting processes to keep pace with the constantly evolving IT environment.

It pays to be a member of DISA — we “pay forward” each day with the deposits we leave behind — great or not-so-great; superior, average, or mediocre. Make no mistake about it, we will be tested and we will be questioned. In the end; however, when we look back upon what we have accomplished, we will see being in DISA was the best thing that could have happened. I relish the thought of being able to depend on the people at DISA with whom I work every day to deliver on their promises and capabilities, and I want you to be able to depend on me.

We will apologize to nobody for our passion to deliver the best joint enterprise capabilities to the warfighter and our mission partners. We will do everything in a skilled and innovative manner, with integrity, precision, and an uncompromising focus to our Core Values, Creed, and Ethos. We will be the premier IT and Cyber Combat Support Agency for the DoD, our nation, and our coalition partners. We are DISA — “United in Service to Our Nation!”

Ronnie D. Hawkins Jr.

RONNIE D. HAWKINS JR.

Lieutenant General, USAF

Director

THE DISA VISION

Information superiority in defense of our Nation.

THE DISA MISSION

DISA, a Combat Support Agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations.

THE DISA ETHOS

United in Service to Our Nation.

CORE VALUES

Dedicated



Integrity



Service



Always



THE DISA CREED

WE are global professionals vital to the defense of our Nation

WE respond to mission priorities with speed and urgency

WE embrace the values and potential of our people

WE engage through a collaborative environment

WE know diversity leads to innovation

WE believe individual growth, learning, and proficiency are critical to our future

WE value perseverance and recognize failure as a growth opportunity

WE build trust through transparency

WE hold ourselves accountable

WE are United in Service

WE ARE



AGENCY FOCUS AREAS

Based upon recent Department of Defense Strategic Guidance, DISA is posturing to support DoD's focus on efforts in the Middle East, Africa, and Pacific regions and will accommodate the communications and information sharing network needs for the Joint Force of the future. As the Department evolves to meet the challenges of today's information environment, so too must DISA evolve. DISA will serve as DoD's early adopter (DISA First) for new enterprise capabilities allowing us to validate the capability meets the stated requirements, identify and resolve any issues with the capability, and demonstrate the operational viability of the capability. With that in mind, DISA's strategic goals and current successes are focused on the following areas:

FOCUS AREA 1 DoD Joint Information Environment (JIE). As the lead for the JIE Technical Synchronization Office (JTSO), we are working with our mission partners to incrementally normalize and synchronize fixed and wireless communications, application rationalization, sun setting legacy systems, and consolidating computing centers to enable a collaborative and secure infrastructure. The JIE will be the secure information framework from which the joint force commander delivers responsive, versatile, and decisive actions on any device, anytime, from anywhere on the globe.

S U C C E S S S T O R I E S : J I E

- Established the first Enterprise Operations Center (EOC) in Europe in July 2013
- Established first Core Data Center (CDC) in Europe in September 2013

FOCUS AREA 2 National Leadership and Nuclear Command, Control, and Communications (NC3) Support. We will focus attention on developing and enhancing enterprise solutions in support of national leadership and NC3. The Joint Systems Engineering and Integration Office (JSEIO) provides a unifying technical authority to ensure Presidential and senior leader communications, NC3, and Continuity of Operations (COOP)/Continuity of Government (COG) mission areas have unified, cost, and operationally effective communications capabilities.

S U C C E S S S T O R I E S : N A T I O N A L L E A D E R S H I P / N C 3 S U P P O R T

- The Strategic and National Command, Control, Communications, and Intelligence (SNC3I) Joint Systems Engineering and Integration Office (JSEIO) was formally established in February 2013

FOCUS AREA 3 Cyber Operations and Mission Assurance. We will posture the Agency in concert with USCYBERCOM to develop a cyber Command and Control (C2) framework; expand DoD Information Networks (DoDIN) Operations (DO) and Defensive Cyber Operations (DCO) mission support through evolving and innovative initiatives like Single Security Architecture (SSA); and by creating an information assurance and cyber trained workforce for better operations within the cyber environment. Additionally, we will establish the JIE operational structures consisting of the Global Enterprise Operations Center (GEOC), geographic and functional Enterprise Operations Centers (EOCs), Core Data Centers (CDCs), and other cyber C2 structures (e.g., Joint Forces Headquarters (JFHQ)), as required, and will support geographic Combatant Commands (COCOMs) with operations and defense of the DoDIN in their respective Areas of Responsibility (AORs).

S U C C E S S S T O R I E S : C Y B E R O P E R A T I O N S / M I S S I O N A S S U R A N C E

- Implemented Enterprise Email Security Gateway which protects in excess of 1.4M user accounts and 2M messages per day
- Implemented the NIPRNet Federated Gateway to mitigate any damages to the NIPRNet and provide the ability to detect attacks sooner

FOCUS AREA 4 Acquisition Agility. DISA will employ an acquisition strategy that reduces procurement cycle times, lowers costs, and accelerates delivery of critical capabilities. Incremental development, preplanned product improvement, enterprise licenses, and agile development will be key in our acquisition strategy.

S U C C E S S S T O R I E S : A C Q U I S I T I O N

- Decreased the cost of Satellite Communications (SATCOM) support for Central Command (CENTCOM) by 34%
- Achieved about \$20M savings in licensing costs for Antivirus contracts
- Set a new record by awarding 29.2% of eligible contracts, totaling \$1.5B, to small businesses in FY13

FOCUS AREA 5 Global Defense Posture. While we will continue to be operationally focused on the current fight in the Middle East and our ongoing engagement efforts in Africa and the Pacific, we will enhance our customer relations management to accommodate and automate where possible to be more agile and responsive to the dynamic changes to our global mission. We will lead the development and operation of a layered, fault-tolerant enterprise information environment consisting of rapidly deployable components that allow for contingency operations in a full range of conflict.

S U C C E S S S T O R I E S : G L O B A L D E F E N S E P O S T U R E

- Implemented an Airborne Intelligence, Surveillance, and Reconnaissance (A-ISR) full motion video (FMV) and imagery dissemination solution supporting U.S. Special Operations Command (SOCOM) and Special Operations Command, Pacific (SOCPAC) requirements under Operation Enduring Freedom, Philippines (OEF-P)

FOCUS AREA 6 DoD Cloud Services. Cloud computing and cloud services offer unprecedented opportunities for cost savings, enhanced information sharing, and mission effectiveness. However, the Department's mission assurance and information interoperability must be maintained, as we take advantage of new and emerging capabilities. As the DoD cloud services broker, we will enable mission partners to tailor the availability and delivery of cloud services from within the Department or from federal or commercial cloud service providers, based on technical and mission requirements. We will also enable rapid provisioning of cloud-based enterprise services, such as Defense Enterprise Email (DEE), Defense Enterprise Portal Services (DEPS), Unified Capabilities (UC), "Big Data" storage and heuristics, virtual desktops, and many other enterprise services for the Department.

S U C C E S S S T O R I E S : D O D C L O U D S E R V I C E S

- Migrated over 4,000 Africa Command (USAFRICOM) and Component personnel to DEE
- Provided a DEPS 2.0 solution for iNavy and its nearly 80,000 users

FOCUS AREA 7 Mobility Initiatives. We will promote rapid delivery, scaling, and utilization of secure mobile capabilities, leveraging commercial mobile technologies that enable an agile deployment environment for new and innovative applications to support evolving warfighter requirements. We will focus on improving three areas critical to mobility: mobile devices, wireless infrastructure, and mobile applications, while also ensuring these areas remain reliable, secure, and flexible enough to keep up with fast-changing technology.

S U C C E S S S T O R I E S : M O B I L I T Y

- Deployed over 1600 Unclassified Devices and 170 Classified Devices to COCOMs/ Services/Agencies
- Delivered an enterprise-wide mobile device manager that ensures a secure operating environment for DoD mobile devices

THE TARGET OBJECTIVE STATE

Our target objective state is an enterprise information environment comprised of a secure connection to a computing environment provided by both commercial and government computing centers and big data storage, interconnected with a mesh of fixed and wireless transport, protected by a single security architecture, whose information resources held in the cloud are reachable by various mobile devices, and accessible by credentialed users eliminating anonymity from the network.

Our next generation IT environment will be dominated by users seamlessly connecting to and through the cloud to access information and enterprise services. Mobility is the primary benefit of JIE. As such, we will posture our networks and peripherals away from wired thin clients and workstations to those that support individual mobile devices with access to the needed resources and information. We will see a shift from traditional hard token credentials to virtual positive identity supported with biometrics. Users will be granted access upon approaching their access point by systems that will immediately recognize the authorized user and grant network access. With JIE as our backbone, we will evolve to truly enable the JIE vision: To connect any credentialed user, via any properly authorized device, to anywhere in the cloud, at any time. Mobility devices are the ultimate access methodology of the JIE.

CHARACTERISTICS OF THE **TARGET OBJECTIVE** STATE

- JOINT INFORMATION ENVIRONMENT
- MOBILE TO FIXED END USER INTEROPERABILITY
- COLLABORATIVE ENTERPRISE SERVICES
- SECURITY INTEGRATED INTO THE CLOUD
- CLOUD CAPABILITIES ENABLED



OUR GUIDING PRINCIPLES

Our mission and responsibilities are global. DISA is required to provide information at Internet speed with available and emerging technologies such that any authorized user can connect to the network with the ability to produce or consume data and services anywhere on the global network.

Our enterprise supports the Defense Department and its mission partners. DISA has been engaged in every mission the Department has undertaken over the decades. These engagements have become increasingly joint, interagency, and international, and our partnerships have increased to reflect this.

We must support the full spectrum of operations. The capabilities and services we provide support information sharing and facilitate decision making no matter the challenges faced and no matter where the information is located or sourced.

We operate in a contested battlespace. Mission success is dependent upon our ability to fight through a concentrated attack while reducing the attack surface, continually improving our command and control of the network, and assuring safe, secure information sharing.

We provide integrated, interoperable, assured infrastructure, capabilities, and services that recognize the enterprise begins at the edge. The edge is where any warfighter or system associated with defense of our Nation is located, and we are committed to the user wherever on the globe they operate.

Our aim is to enable and ensure end-to-end service. We and our mission partners are engaged from user to user – from wherever information is produced to wherever it is consumed.

The DISA enterprise must be always-on. The capabilities and services DISA provides are expected to be on and available to users 24x7x365.




The DISA Strategic Goals

There are four strategic goals in this plan. These goals and the supporting key objectives link our strategy to our day-to-day operations and guide us in building the DISA of tomorrow.

JOINT INFORMATION ENVIRONMENT

The JIE will be the secure information framework from which the Joint Force Commander delivers responsive, versatile, and decisive actions on any device, anytime, from anywhere on the globe.

STRATEGIC GOAL 1  **Evolve the Joint Information Environment.** Evolve a consolidated, collaborative, and secure joint information environment, enabling end-to-end information sharing and interdependent enterprise services across the Department that are seamless, interoperable, efficient, and responsive to joint and coalition Warfighter requirements. **FOCUS AREAS 1, 3, 5, 6, 7**

Key Objective 1.1: Implement and sustain an efficient, converged, and consolidated IT infrastructure accessible by all means from any authorized user, anywhere within the DoD.

- ▲ Normalize Networks with common standards with the intent to eliminate excess redundancy and legacy non-Internet Protocol (IP) services to create a unified capabilities, everything over IP meshed transport infrastructure
- ▲ Standardize and consolidate computing infrastructure to maximize utilization of fiscal resources and offer better valued services to mission partners, through Cloud Broker managed arrangements
- ▲ Synchronize all efforts with the JTSO to ensure proper execution of JIE increments
- ▲ Establish the JIE CDCs leveraging the Defense Enterprise Computing Centers (DECCs)

Key Objective 1.2: Develop Joint Enterprise Mission Assurance Solutions that expand and extend the security protections of the Department's information assets focusing on solutions and capabilities, while enabling authorized users to productively access needed information using any device and from anywhere in DoD.

- ▲ Implement Identity and Access Management (IdAM) to enable secure access and eliminate anonymity from the network
- ▲ Using the SSA, harden the network infrastructure, enclave, and host environments from cybersecurity threats by deploying the Joint Regional Security Stacks
- ▲ Enable cyber security while focusing on enhanced mobility requirements of the enterprise

Key Objective 1.3: Provide a portfolio of optimized and integrated enterprise service offerings that enable DoD-wide efficiencies and effectiveness, and improved responsiveness to dynamic joint and coalition mission partner needs.

- ▲ Employ a "DISA First" philosophy for piloting emerging enterprise services prior to expanding delivery beyond DISA boundaries
- ▲ Expand delivery of enterprise services (i.e. milCloud, DEE, DEPS, and UC) to all Services, Agencies and activities
- ▲ Deliver foundational services (i.e., metadata registry, content delivery, identity management, joint user messaging, etc.) to provide a common core of infrastructure services that are critical to higher level services, re-usable components, and applications
- ▲ Establish a "Big Data" capability to handle the storage and analysis of data in excess of exabyte capacities
- ▲ Establish an Airborne – Intelligence, Surveillance, and Reconnaissance (A-ISR) Transport Service

Key Objective 1.4: Promote rapid delivery and utilization of secure mobile capability, leveraging commercial mobile technology to enable an agile deployment environment for new and innovative applications to support evolving warfighter requirements.

- ▲ Establish common infrastructure and services for both unclassified and classified mobile solutions to enable the efficient application of mobile technologies to meet a wide range of DoD requirements
- ▲ Establish security standards and a certification process sufficiently agile to keep pace with the rate of evolving mobile technologies
- ▲ Provide a framework for management of applications to expand the capabilities available to users via mobile technology

Key Objective 1.5: Provide a full array of electromagnetic spectrum services and capabilities ranging from short-notice on-the-ground operational support at the forward edge to long-range planning.

- ▲ Pursue national and international strategic objectives to ensure DoD's access to spectrum in support of warfighting capabilities with a view towards efficient, flexible, and adaptive technology
- ▲ Enhance quality and timeliness of operational spectrum management (SM) support for warfighting operations
- ▲ Lead the development of comprehensive and integrated strategic and implementation plans, and an architecture to transform SM to support future cloud based operations and warfare
- ▲ Perform SM and engineering analyses supporting national and international spectrum use initiatives to ensure DoD spectrum access
- ▲ Implement, integrate, and improve cloud-based SM services/capabilities and influence/facilitate the implementation of emerging spectrum technologies



STRATEGIC GOAL 2 Provide Joint Command and Control (JC2) and Leadership Support.

Engineer, provide, and enhance C2 and mission partner information sharing capabilities to enable decision makers with the ability to exercise authority and direction over assigned and attached forces and resources, while rapidly and effectively sharing information across the strategic, operational, and tactical spectrum of operations. DISA will lead the development and evolution of JC2 capabilities used to plan and execute the full range of joint, interagency, and multinational military operations.

FOCUS AREAS 2, 5

Key Objective 2.1: Develop and enhance capabilities to better engineer, integrate, and operate national leadership enterprise solutions.


- ▲ Through the JSEIO, perform end-to-end system engineering to modernize and enable reliable interoperable NC3 national and senior leadership communications; and continuity communications
- ▲ Support White House Communications Agency (WHCA) and White House Situation Support Staff (WHSSS) communications systems modernizations and crisis management activities, in order to provide the ability for our national leadership to effectively coordinate, make decisions, and respond rapidly during times of stress and national emergency

Key Objective 2.2: Evolve the JC2 architecture and deploy its associated C2 enterprise capabilities.

- ▲ Modernize the Global Command and Control System–Joint (GCCS-J) global baseline, Joint Planning and Execution System (JPES), and Global Combat Support System–Joint (GCSS-J) to network based solutions in accordance with the JC2 objective architecture
- ▲ Expand the use of widget development and delivery approach across the C2 portfolio

Key Objective 2.3: Develop and integrate Multi-National Information Sharing (MNIS) material solutions as a foundation for the Mission Partner Environment (MPE).

- ▲ Assist with the development of MPE operational concepts as the requirements drivers for integrated mission partner information technology (IT) capabilities
- ▲ Migrate the existing Rel-Secret capabilities to a more efficient infrastructure and set of common services
- ▲ Deliver and evolve the enterprise unclassified information sharing service

STRATEGIC GOAL 3  **Operate and Assure the DISA Information Enterprise as a part of the Department of Defense Information Networks (DoDIN).** Command and control, plan, direct, coordinate, integrate, and synchronize the DoDIN Operations (DO) and select Defensive Cyber Operations (DCO) to secure, operate, defend, and protect the DoDIN across the full spectrum of military operations. Through our partnership with USCYBERCOM, evolve our cyber and network capabilities to function under dynamic conditions responding to increasing warfighter information requirements, increased demand for operational efficiencies, and shifts in the global defense posture. Organize to consistently and rapidly adapt to changing circumstances around the world on demand, using advanced technologies and standardized tool sets, synchronized processes and procedures, and a highly trained cyber workforce. **FOCUS AREAS 1, 3, 5**

Key Objective 3.1: Operate and assure a reliable, available, resilient, secure, and protected global net-centric enterprise in direct support of joint and coalition warfighting.

- ▲ Execute 24x7 day-to-day operations, management, and assurance across network, computing, enterprise and C2/information services, and communications environments under DISA Operations
- ▲ Implement a unified organization for operating and assuring the DISA information enterprise under a single operational structure to optimize service operations and defensive cyber operations to support the evolution to JIE
- ▲ Continue to mature and develop the Operational Support Systems (OSS) (i.e., tools) and tactics, techniques, and procedures (TTPs) to improve the delivery of DISA provided services
- ▲ Establish a Cyber C2 Framework and a Joint Force Headquarters (JFHQ) in support of USCYBERCOM for executing operations and defense of the DoDIN
- ▲ Establish and mature the JIE operational structures in DISA: GEOC (potentially), geographic and functional EOCs, and CDCs
- ▲ Operationalize Cyber Protection Teams (CPTs)

Key Objective 3.2: Evolve DISA policy, processes, and procedures to better support operations, sustainment, standardization, and interoperability to achieve operational effects across the DoDIN and JIE.

- ▲ Expand Network Operations (NetOps) governance, institutionalizing common procedures and standards, for effectively inserting, operating, and defending capabilities in the DISA enterprise
- ▲ Mature a framework to optimize service delivery and operations and provide a common understanding of how emerging technologies integrate into the enterprise
- ▲ Integrate operational readiness with Agency governance structures to inform Agency priorities of risk and associated remediation
- ▲ Develop and institute Agency-wide configuration management processes and supporting tools
- ▲ Optimize contract transitions and contract lifecycle management practices, emphasizing methods for measuring, monitoring, and managing performance-based contracts, to prevent loss of operational capabilities or readiness
- ▲ Complete military construction (MILCON) and achieve operating capability at new CONUS-based facilities by FY2016

Key Objective 3.3: Assess, shape, and influence the Agency's readiness posture to ensure the Agency is capable of meeting warfighting requirements including optimizing and exercising contingency operations and protecting critical infrastructure.

- ▲ Conduct, evaluate, and enhance COOP, Critical Infrastructure Protection (CIP), and Defense Industrial Base (DIB) activities
- ▲ Utilize "Big Data" analytics and heuristic capabilities to strengthen cyber operations and cyber protection capabilities to better defend the network
- ▲ Continuously improve DISA's Readiness Program, adjusting Mission Essential Tasks (METs) and performance measures/metrics to reflect mission requirements, to know, understand, and accept risk and resource implications
- ▲ Evolve and reshape the operations workforce through training programs, hiring strategies, and other developmental methods to meet the demands of new enterprise technologies and cyberspace operations. This includes enhanced use of cyber ranges and actively leading/participating in DoD and coalition exercises


Key Objective 3.4: Optimize mission partner engagement to anticipate, influence, and respond to DoD mission requirements.

- ▲ Enhance DISA's outreach efforts enabling both headquarters and field personnel to accurately and concisely promote current and planned DISA services, and improve responsiveness to mission partners' emerging requirements (e.g. Integrated Priority Lists (IPLs), COCOM Campaign Plans)
- ▲ Foster partnerships with our mission partners, private industry, other federal departments and our allies to exchange information and strengthen cyber security strategies
- ▲ Enable crisis/contingency operations for the DoDIN worldwide
- ▲ Transition responsibilities for the Afghanistan Telecommunications Advisory Team (TAT) to the U.S. Department of State by FY2015

CYBER OPERATIONS

We will develop and train cyber security professionals for proactive cyber defensive operations.



STRATEGIC GOAL 4  **Optimize Department Investments.** Enable the Department to maximize use of its resources by providing cost efficient capabilities; an effective and defensible infrastructure; and standardized support services, business processes, and policies that enable the rapid infusion of technology into the enterprise.  **FOCUS AREAS 3, 4, 5, 6, 7**

Key Objective 4.1: Promote the implementation of acquisition and procurement policies, processes, and practices that enable the development of the enterprise concept and provide agile enterprise IT contract solutions for the Department.

- ▲ Streamline Agency acquisition and contracting processes to support the enterprise
- ▲ Manage existing Agency contracts to eliminate duplication, optimize service offerings, and gain enterprise-level efficiencies to ensure “best value”
- ▲ Manage mission partner requirements to achieve strategic sourcing cost and performance efficiencies, and maximize Enterprise License Agreements (ELAs)
- ▲ Expand cloud broker services for the Department facilitating and optimizing access to government and commercial cloud services that can meet security and interoperability requirements, ensure that new services are not duplicative within the Department, and consolidate cloud service demand at the enterprise level
- ▲ Maximize mobile communication capabilities by fielding a portfolio of innovative mobility contracts
- ▲ Develop and deploy innovative contracting strategies to acquire commercial Cloud Service Provider (CSP) solutions

Key Objective 4.2: Demonstrate fiscal responsibility in every aspect of our operations.

- ▲ Ensure transparency of DISA’s financial resources
- ▲ Effectively align resources to evolving mission requirements and contingency operations
- ▲ Implement standard business processes and models to define the enterprise capabilities and service offerings of the Agency and ensure continued value to the Department
- ▲ Implement property accountability enhancements to tighten controls and eliminate losses of accountable items

Key Objective 4.3: Align and optimize our workforce and DISA infrastructure to address increasing cybersecurity mission needs.

- ▲ Effectively position our assets where they can be best utilized to support cyber mission needs
- ▲ Cultivate a highly-capable workforce characterized by agility, flexibility, and diversity
- ▲ Establish a strong cyber defense workforce component
- ▲ Establish an operationally focused cyber training program, leveraging information assurance (IA)/cyber standards, which will prepare DoD cyber professionals to operate and defend our networks in an increasingly threat-based environment
- ▲ Support the USCYBERCOM Cyber Security Inspection Program (CSIP), along with optimizing other IA inspection and certification efforts, such as the Command Cyber Readiness Inspection (CCRI) Program, to evaluate operational readiness and mission impact based on implementation of an effective cyber security posture
- ▲ Expand and hone cyber defense services and support to ensure integral CND services for future DoD enterprise services and coalition networks

Key Objective 4.4: Evolve the DoD's development, test, certification, deployment, and sustainment lifecycle to accelerate capability delivery and reduce lifecycle costs.

- ▲ Provide and extend the Forge.mil service to support collaboration, automated testing, and certification of applications
- ▲ Provide efficient, responsive interoperability testing, and test, evaluation, and certification (TE&C) capabilities and environments as a service
- ▲ Deliver on demand infrastructure and platform as a service (IaaS, PaaS) integrated with Forge.mil to enable continuous application delivery

Key Objective 4.5: Clearly communicate the Agency strategy, and available DISA services and capabilities to inform the Department of DISA's offerings, both internal and external to the Agency.

- ▲ Transform National and Department-level direction and policy into an Agency Strategic Planning Guidance
- ▲ Enhance DISA's social media and outreach capabilities with timely, relevant and informative information
- ▲ Implement a single Agency request fulfillment process and toolset that is seamlessly integrated with DISA's service catalog





Technology for the War Fight

The services that DISA provides — communications, networking, cyber security, and information services — are evolving more rapidly than almost any sector of the economy. Mobile and cloud computing technologies are globally transforming our operational landscape, enabling greater mission effectiveness through improved communication, access, information sharing, and action response time. The evolution and influx of these and other new technologies onto the commercial marketplace is occurring at an unprecedented pace. In parallel is the warfighters' growing need for information superiority across the spectrum of operations and within the contested battlespace of the cyber domain. The landscape is changing, there are more devices than people in this world; devices, inventory, facility controls, and even human i are addressable and connected to systems and networks. DISA's ability to effectively support the IT needs of the warfighter is predicated upon our ability to keep pace with the technology within this sector.

Rapid adoption and integration of new technologies is not without challenges. Current timelines associated with certification and accreditation processes and the need for rigorous security controls must be managed. Application Lifecycle Automation technologies promise to substantially reduce the time from initial application development to its delivery in the field. DISA will mitigate these barriers utilizing best practices to streamline business processes; anticipating the Department's demand for services and the capacity to meet those demands; and implementing a technology strategy that provides new, less expensive and improved technical capabilities that meet warfighters changing needs.

TODAY

Our talents are focused on the near-term requirements of our mission partners and the Department's vision of an enterprise information environment, to include the following:

- ▲ Converged, integrated, and enhanced enterprise infrastructure
- ▲ Improved networks, communications, and interoperability for better information sharing and collaboration
- ▲ Faster, more responsive delivery of capabilities and adoption of commercial IT
- ▲ Improved security to reduce cyber threats

TOMORROW

DISA's ability to anticipate and meet the demands of our users will be based on identification and characterization of technological advancements that hold future relevance and benefit to the Department. Posturing for success, DISA has established a Strategic Technology Watchlist — a set of key focus areas based on mission partner priorities — where the associated technologies are the most critical for DISA to understand, acquire, and evolve over the next five years. DISA will effectively manage the identification, acquisition, adoption, and insertion of advanced technology into DISA systems and operations, and employ robust techniques of technology evaluation and characterization, experimentation, and piloting. The ability to conduct focused evaluations, experiments, and piloting activities is critical to the successful integration of these technologies and realization of the resulting operational capacities.



MOBILITY

Mobility devices are the ultimate access methodology of the JIE.

2014 – 2019 TECHNOLOGY WATCHLIST

Agile and Adaptive Command and Control (A2C2) Technologies. Refers to technologies that enable the evolution from net-centric to mission-centric capabilities for the purpose of establishing decision superiority. Mission-centric implies moving data to decisions, spontaneously assembling the components that are best suited for the required mission decisions and dynamically suggesting viable decision alternatives both in mission planning and execution. A2C2 must leverage several of the technologies within this watchlist, as well as mission process modeling technologies. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 2 (Provide Joint C2 and Leadership Support).

Application Lifecycle Automation Technologies. Refers to technologies that can fully automate the process of ordering and provisioning computing resources; building and patching applications; locking down, scanning, and remediating; testing and progressing from development to test to operations; and continuously monitoring and ensuring applications are healthy and free of security issues. Since there is a dire need among the DoD community to speed advanced capabilities to the field, DISA must address the process bottlenecks and provide an integrated suite of capabilities designed to drive agility into the development, deployment, test, and maintenance of secure Department of Defense (DoD) applications, and deliver cloud services tailored to DoD information system requirements. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 4 (Optimize Department Investments).

Data Services (Big Data) Technologies. Refers to technologies that can leverage massively parallel, commodity computing, and storage for analyzing massively large and complex data sets. Big Data capabilities are becoming essential to modern warfare, and DISA needs to be able to provide Big Data capabilities to its mission partners. Big Data allows for deploying processing to the data, especially where the data is too big to move over existing and emerging networks, and enables the analysis of trends and identification of anomalies. The improvements in effectiveness and efficiency of data exploitation are vital in keeping ahead of our adversaries world-wide. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), and Strategic Goal 3 (Operate and Assure the DISA Information Enterprise).

Cloud Computing Technologies. Refers to technologies that allow service providers to provide self-service, on-demand, and rapidly elastic computing resources (e.g. computing capacity, storage, computing platforms, virtual desktops, and enterprise applications) to third party consumers. As the lead provider of Cloud Computing services for the Department, DISA must ensure its offerings provide the most advanced and flexible capabilities in order to ease the burden of migrating applications resulting from federal guidance to consolidate data centers. The Department's realization of future cloud computing capabilities, including public, private, commercial, and DoD, requires innovative cloud management and orchestration services. These services will speed the provisioning of services across multiple clouds, enable the simultaneous operation of multiple clouds, and allow rapid migration of workloads between clouds. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), Strategic Goal 3 (Operate and Assure the DISA Information Enterprise), and Strategic Goal 4 (Optimize Department Investments).

B I G D A T A

Big Data capabilities are becoming essential to modern warfare, and DISA needs to be able to provide Big Data capabilities to its mission partners.

Cyber Command and Control (C2) Technologies. Refers to technologies that can provide cyber behavior monitoring, analytics, situational understanding, and C2 of the emplaced computing, networking, and security apparatus. As the operator of the DoDIN, it is crucial that DISA provide exhaustive, proactive, and continuous mission assurance to all network components starting from initial technology and software supply chain, running through operations, and ending with appropriate technology disposal. The maturation of these technologies and the integration of the resulting capabilities are keys to achieving Strategic Goal 3 (Operate and Assure the DISA Information Enterprise).

Enterprise Identity and Access Management Technologies. Refers to the capability for positively identifying users (people or software) that operate on the DoDIN and managing the access of the users to network resources and services. DISA must provide comprehensive, reliable, and consistent capabilities to bind user activity to their digital identities and ensure access to authorized resources is carefully controlled. These capabilities reduce the risk of insider/outsider threat by binding access control activity to digital identities to ensure all users are strongly authenticated, access is limited to authorized resources, and all users may be monitored. The maturation of these technologies and the integration of the resulting capabilities are key to achieving the Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), and Strategic Goal 3 (Operate and Assure the DISA Information Enterprise).

High Performance Networking Technologies. Refers to technologies that will allow network backbones to achieve capacities of 100 Gbps or greater. While capacity improvements to wireless/satellite networks will undoubtedly be more modest, the need for spectrum and bandwidth will still be high, particularly close to areas of conflict. For example, a growing number of Aerial (Airborne) Intelligence, Surveillance, and Reconnaissance (A-ISR) assets require increased capacity, global coverage, and sustainment plans to support this growing mission. Additionally, with the move to enterprise and cloud computing, improving the performance of DISA's network backbone provides enhanced management and provisioning capabilities that enable rapid and efficient scaling of bandwidth, while minimizing manual upgrades to field components. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment) and Strategic Goal 3 (Operate and Assure the DISA Information Enterprise).

Secure Mobile Technologies. Refers to devices and applications that are intended to be securely used by mobile users within DoD. The potential operational impacts of using mobile computing across DoD are great. DISA must seek to overcome the legitimate security issues and tremendous scalability of mobile computing demand. The maturation of these technologies and the integration of the resulting capabilities are key to achieving Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), and Strategic Goal 3 (Operate and Assure the DISA Information Enterprise).

The Internet of Things. Refers to the commercial trend of connecting uniquely addressable “smart” devices and sensors to a wide area network. The rapid growth of technologies and products support in this realm will result an explosion of capabilities on our sensitive unclassified and classified networks. This will provide multiple new sources of data (driving the need for Big Data technologies) as well as enhanced control of the virtual and physical world. From improved logistics tracking, to optimized building security and environmental controls, to health monitoring of individual soldiers, the Internet of Things will impact everything we do. At the same time it will introduce new cyber challenges we must be prepared to meet. As such, the Internet of Things will help us achieve (or have impact upon) Strategic Goal 1 (Evolve the Joint Information Environment), Strategic Goal 2 (Provide Joint C2 and Leadership Support), Strategic Goal 3 (Operate and Assure the DISA Information Enterprise), and Strategic Goal 4 (Optimize Department Investments).

These nine focus areas constitute a progression of the technology set for the watchlist derived from COCOM IPLs and the needs of DISA's mission partners and directorates.

BEYOND

It is imperative that we look beyond the technologies of tomorrow. We must anticipate the future capability demands of our users and how emerging technologies can be brought to bear on these critical operational challenges. DISA must maintain a strong presence in the Science and Technology (S&T) communities, and we must effectively influence technological research and investment. This will ensure that DISA has awareness of the relevant game-changing or disruptive technologies and shape these technologies to the unique challenges of the DoD. Truly disruptive technologies allow us to realize a multiplier in terms of cost savings, time savings, resource savings, operational effectiveness, better security, and enhanced cyber protection. Recent examples include server virtualization, wirelessly connected tablet computers, and cloud computing.

DISA's partnerships with industry, academia, and our mission partners are critical to forecasting these emerging technologies and their value to the Department, and supporting informed technology investment decisions that will strengthen the enterprise and improve the enterprise service capabilities we ultimately deliver.

CLOUD SERVICES

Cloud computing and cloud services offer unprecedented opportunities for cost savings, enhanced information sharing, and mission effectiveness.





Conclusion

As a Combat Support Agency, we are committed to providing only our very best efforts to enable the immediate connection, sharing, and assured access to information capabilities for our mission partners. This strategic plan describes DISA's fundamental goals as well as the key objectives that form the core of our commitment — our high level strategy to deliver JIE to the warfighter.

The cornerstone of our warfighter support remains our Agency's people and the leadership's desire to proactively posture for the future during the Department's fiscally challenged and resource constrained operational environment. DISA is confidently pursuing courses of action that set the stage to identify the most relevant advances in technology and to deliver capability for the warfighter.

We will continue to reorganize and reposition resources to meet the needs of the Departments — essentially JIE and our enterprise requirements. Today, under the auspices of JIE, we have virtualized services in the cloud. Tomorrow, we will evolve the security architecture to address certification and accreditation reciprocity; we will deliver unified capabilities; and finally, we will become pivotal to the Big Data efforts of the Department. Rest assured, we are committed to our mission partners' success. **DISA**

MOBILITY

COLLABORATION

CYBER

BIG DATA

CLOUD



www.disa.mil



PUBLISHED 7 MAY 2014